УДК 338.1

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В СФЕРЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ

О. С. Маковоз
профессор кафедры менеджмента и налогообложения,
доктор экономических наук, доцент,
Национальный технический университет
«Харьковский политехнический институт» (Украина)
e-mail: mosua@meta.ua

Аннотация. *Охарактеризована экономическая безопасность в сфере электронной коммерции как стабильное состояние системы в условиях экономического развития. Исследованы основные причины преступлений и угроз экономической безопасности в электронной коммерции. Предложены возможные направления решения задачи построения комплексной системы защиты от преступлений и угроз в электронной коммерции.*
Ключевые слова: *экономическая безопасность, электронная коммерция, компьютерные преступления, технические средства, угрозы.*

Annotation. *Economic security in e-commerce is described as a stable state of the system in the context of economic development. The main causes of crimes and threats to economic security in e-commerce have been investigated. Possible directions of solving the problem of building a comprehensive system of protection against crimes and threats in e-commerce are proposed.*
Keywords: *economic security, e-commerce, computer crime, technology, threats.*

В условиях цифровой экономики уровень развития любого государства определяется обоснованной и целесообразной политикой, направленной на обеспечение экономической безопасности в условиях распространения использования цифровых технологий. Трудно представить современное общество без интернет-трансакций и электронной коммерции. При этом в процессе электронной коммерции возникает множество разнообразных угроз, связанных с организационными, правовыми и финансовыми проблемами в безопасности экономической деятельности. Под экономической безопасностью следует понимать стабильное состояние системы в условиях экономического развития. Наиболее распространенными причинами преступлений и нарушения безопасности в электронной коммерции являются: сетевые атаки; атаки на пароли и системы аутентификации пользователя; ошибки, сбои и отказы программно-технического обеспечения системы электронной коммерции (далее — СЭК); вредоносные программные защиты; фальсификация; ошибки и другие непреднамеренные действия обслуживающего персонала СЭК.

Основными источниками угроз СЭК являются:

непреднамеренные угрозы, вызванные стихийными и техногенными катастрофами случайного характера, нарушающих непрерывность бизнес-процессов, доступность данных и сервисов СЭК, целостность данных;

ошибки пользователей и обслуживающего персонала СЭК;

преднамеренные действия злоумышленника, направленные на нарушение таких составляющих информационной безопасности, как доступность, целостность и конфиденциальность информации, циркулирующей в СЭК [1, с. 83].

Обеспечение экономической безопасности в сфере электронной коммерции — серьезная и непростая проблема, поскольку эта сфера молодая, много организационно-правовых отношений еще только формируются и закрепляются, компьютерные преступления сложнее выявить и раскрыть, что объясняется высокой квалификацией самих преступников, трудностью сбора доказательств и, следовательно, доказывания виновности подозреваемого, возможностью совершения преступления фактически с любой точки планеты с использованием систем удаленного доступа, Интернета и т. п. [2, с. 83].

Правовое регулирование электронной коммерции в Украине осуществляется Гражданским кодексом, Законом Украины «Об электронной коммерции» и другими законодательными актами. В то же время такие сферы, как электронные платежные системы, таможенное оформление и налогообложение, конфиденциальность, безопасность, защита интеллектуальной собственности, требуют совершенствования правового регулирования. По оценкам группы экспертов компании EVO, украинцы стали больше покупать товаров и услуг — в 2019 году экономика страны показывает высокие темпы роста ВВП (4,2 % по итогам трех кварталов) прежде всего за счет розничной торговли. По данным Госслужбы статистики Украины, за 11 месяцев 2019 года розница прибавила 11,3 % или почти в 2,5 % раза больше, чем вырос ВВП. При этом проявилась новая тенденция: торговля уходит в онлайн. То есть намного быстрее, чем традиционные продажи, росла в 2019 году интернет-торговля. Все больше покупателей предпочитают делать покупки онлайн, не заходя в магазины [3].

Одно из самых важных условий для эффективного использования системы электронной коммерции — обеспечение эффективного, недорогого и безопасного средства проведения платежей. Известно достаточное количество способов коммуникаций в сети Интернет. Популярной сейчас становится криптография с отрытым ключом. Выбор лучших средств защиты платежей должен быть поручен специалистам. Организация электронной коммерции должна базироваться на использовании традиционных юридических норм и правил, предусматривать разработку новых специализированных институтов и процедур.

First Atlantic Commerce (далее — FAC) — международная организация, обеспечивающая безопасный онлайн-платежный шлюз для организаций во всем мире. В рамках процесса проверки заказов FAC предоставляет услуги проверки адреса (AVS) и удостоверение личности с картами (CVC), включая CVV2 для Visa MasterCard и CID для American Express. Благодаря сервису продавцы могут автоматически отображать и обрабатывать транзакции через платформу в режиме реального времени, что позволяет им немедленно действовать в случае возможного мошенничества с CNP. Сервисы 3D-Secure предоставляют возможность проверять настоящую личность своих потребителей с помощью безопасного процесса аутентификации плательщика, который является владельцем определенной карточки. Следует отметить, что активно внедряется в работу банков веб-отчетность, которая позволяет видеть отклоненные транзакции [4].

Таким образом, можно сделать вывод, что только технических средств для решения задачи построения комплексной системы защиты от преступлений и угроз в электронной коммерции недостаточно. Необходимо внедрять политику безопасности электронной безопасности с применением целого комплекса организационных, законодательных, физических и технических мероприятий. Целесообразно в системе электронной коммерции применения организационных, программно-аппаратных, технических средств защиты информации. Следует заметить, что вышеприведенные методы защиты должны базироваться на нормативно-правовой основе, которая станет фундаментом в решении вопросов обеспечения экономической безопасности в сфере электронной коммерции.

1. Оладько В. С. Модель действий злоумышленника в системах электронной коммерции // Международный научно-исследовательский журнал. 2015. № 7–1 (38). С. 83–85. Вернуться к статье

2. Смирнова Л. Я. Анализ основных видов преступлений в сфере электронной коммерции // Закон и право. 2007. № 2. С. 83–84. Вернуться к статье

3. Украинцы уходят в онлайн: что народ покупает в интернете и почему растут цены [Электронный ресурс]. URL: https://cross-media.org.ua/rticles/ukraincy-uhodyat-v-onlayn-chto-narod-pokupaet-v-internete-i-pochemu-rastut-ceny (дата обращения: 22.02.2020). Вернуться к статье

4. All-in-one e-commerce fraud guide: types, definition, prevention 2018 [Электронный ресурс]. URL: https://amasty.com/blog/all-in-one-e-commerce-fraud-guide-types-detection-prevention-2018/ (дата обращения: 22.02.2020). Вернуться к статье